

出國報告（出國類別：進修）

損壞航電晶片解讀 在職訓練出國報告

服務機關：飛航安全調查委員會

姓名職務：副工程師／陳沛仲

派赴國家：俄羅斯莫斯科市

出國期間：民國 107 年 7 月 29 日至 8 月 4 日

報告日期：民國 107 年 10 月 24 日

目次

一、目的	2
二、排定行程	3
三、訓練過程	7
四、心得及建議事項	23

一、目的

近年來，我國已發生多件普通航空業、公務航空器及超輕型載具的飛航事故，從 2016 年 1 月至 2018 年 8 月期間飛航安全調查委員會（以下簡稱本會）所調查的 21 件飛航事故之中即有 12 件屬此類事故，此類航空器多未安裝飛航紀錄器，事故調查需仰賴機上手持式全球衛星定位系統接收機（Portable GPS）或電子飛航儀表系統（EFIS）等航電裝備。此類航電裝備因不具備飛航紀錄器等級的抗墜存活規格，常因事故時之撞擊而損壞，如何處理損壞航電裝備並解讀關鍵資訊在全球飛航事故調查領域皆為一新興的調查技術。

本會自 2009 年起開始建立損壞 Portable GPS 航電晶片之解讀能量，至今已與台灣國際航電公司（Garmin）、法國飛航事故調查局（BEA）及俄國國際航空委員會（IAC）等機關構建立合作管道，建立解讀 Garmin GPS 裝置之軟硬體能量，至今除應用於本國飛航事故調查之外，並協助日本運輸安全委員會（JTSB）解讀該國普通航空業飛航事故損壞之 Garmin GPS 裝置。

然隨著電子科技日新月異，航電晶片隨著記憶體容量、讀寫速度的增加之外，其讀寫機制亦愈趨複雜，本會現有能量已不足以應付國內普通航空業甚至超輕型載具上搭載的新式航電裝置，近年來亦有事故現場取回之損壞大容量記憶晶片無法解讀之情形，相關軟硬體能量皆極待提升，適逢俄國 IAC 於 2017 年完成新實驗室的建置，相關能量更加提升，故本會近年與 IAC 積極接洽相關在職訓練事宜，派遣本會實驗室損壞晶片相關技術人員前往受訓。

在職訓練方式為期 3 天，著眼於認識 IAC 損壞航電裝置的解讀能量並實際操作損壞航電裝置解讀過程。課程包含：損壞航電裝置清潔、損壞檢測、記憶晶片型號確認、解焊及植球作業、治具匹配、損壞電路修復、原始資料下載、共同發展損壞航電晶片解讀系統，以及案例研討。

授課講師 Alexander Dyachenko 現為 IAC 飛航事故調查科學與技術支援委員會副主席，有 20 年以上之損壞航電晶片解讀經驗，並親自開發多款損壞航電晶片解讀工具無償提供與各國飛航事故調查機關使用，本會近年來多利用其開發之解讀工具針對事故機損壞航電裝置進行資料解讀作業。

二、排定行程

日期	起訖地點	任務
7/29 ~ 7/30	台北-莫斯科	啟程
7/31 ~ 8/2	莫斯科	在職訓練
8/3 ~ 8/4	莫斯科-台北	返國

訓練課程主題：損壞航電晶片解讀訓練（課程如下）

● INTRODUCTION（簡介）

- Overview of IAC Laboratory Workspace（IAC 實驗室作業環境介紹）
- Satellite Navigation Technology overview（衛星導航科技概觀）
- WGS 84 coordinate system（WGS 84 座標系統介紹）
- TrackLog function and its main modes（軌跡記錄程式及其主要模式）

● UNDAMAGED DEVICES（未損壞航電裝置處理）

- Downloading data（下載資料）
- TrackLog data to FDR data（從軌跡紀錄資料至 FDR 資料）
- Calculation of unregistered flight parameters (speed, bank angle, true altitude, heading, etc.)（未紀錄飛航參數之計算(速度、坡度、真實高度或航向等)）
- Representing flight data: use of Geographic Information System and Flight Data processing software（展示飛航資料：利用地理資訊系統及飛航資料處理工具）
- Identification of inadequate track fragments（不合理航跡辨識）
- Interpolations: smoothing techniques（內積：航跡平滑化技巧）

● DAMAGED DEVICES（損壞航電裝置處理）

- Type of damages（損壞情形分類）

- Main types of memory chips packages (TSOP, BGA, FBGA, etc.) (主要記憶體晶片封裝(TSOP, BGA,FBGA 等))
- Hard reset issue (強制重啟問題)
- PCB inspection (電路板檢視)
 - ◆ Optical (光學檢視)
 - ◆ X-Ray (X 光掃瞄)
- Technology of memory chips extraction from PCB (電路板記憶體晶片取下技術)
- BGA reballing technology (BGA 晶片植球技術)
- Retrieving chip dump (抽出晶片原始資料)
- **ANALYSIS OF RAW MEMORY DUMPS (原始資料分析)**
 - HexView program overview (HexView 應用程式概觀)
 - HexView main tools (HexView 主要工具模組)
 - ◆ Big files truncate (大型檔案切割)
 - ◆ Cursor value decoding (游標數據解碼)
 - ◆ Navigation and auto-scheme of memory dump (原始資料之索引及自動處理方案)
 - ◆ Searching and highlighting (搜尋及標記功能)
 - text values in different coding pages (不同編碼檔案中之文字數值)
 - numbers (floating point values) (浮點數數值)
 - date and time values (日期與時間數值)
 - HexView: Flight data decoding (HexView 飛航資料解碼)
 - ◆ Expert identification of tracklog data structure technology (軌跡紀錄資料結構之專業鑑識技術介紹)
 - ◆ Internal database of tracklog data structure (軌跡紀錄資料結構之內建資料庫)
 - ◆ Automatic tracklog data decoding function (軌跡紀錄資料自動解碼功能)

- ◆ Analysis of waypoint data (導航點資料分析)
- ◆ Saving result in GPX format (儲存結果為 GPX 格式)
- File system analysis (檔案系統分析)
 - ◆ File system technology overview (檔案系統科技概觀)
 - ◆ HexView.FAT program overview (HexView.FAT 解讀程式概觀)
 - ◆ Reconstructing logical drive hierarchical tree (folder and files tree) (重新建立邏輯磁碟階層(資料夾與檔案樹))
 - ◆ Extracting data from logical drive dump (自邏輯磁碟原始檔取出資料)
- **RECOVERING DATA FROM DAMAGED MEMORY CHIPS (損壞記憶體晶片資料回復)**
 - Design of FLASH memory (快閃記憶體設計簡介)
 - Retrieving raw memory dump by JTAG interface (透過 JTAG 介面存取記憶體原始資料)
 - Extracting chip die (取出晶體)
 - Building new interconnections with extracted die (對取出晶體之損壞電路進行新建電路修復作業)
- **PRACTICAL PART (實作)**
 - PCB inspection (電路板檢視)
 - BGA chip extraction (BGA 晶片取下)
 - Raw data analysis – HexView (以 HexView 分析原始資料)
 - Reballing (晶片植球)
 - Mounting BGA chip back to the device (安裝 BGA 晶片回裝置)
 - X-Ray inspection (X 光檢視)
 - Flight data processing (飛航資料處理)



圖 1 參訓學員及講師於 IAC 門口合影

三、訓練過程

茲將本次訓練重點摘要如後。

3.1. IAC 實驗室組織概況、作業環境及裝備簡介

州際航空委員會（Interstate Aviation Committee, IAC）為俄國及獨立國協加盟國之民航主管機關，事故調查相關的部門包括執掌事故調查的飛航事故調查委員會（Air Accidents Investigation Commission）及執掌紀錄器解讀、現場測量、飛安研究及工程技術支援的飛航事故科學與技術支援委員會（AAI Scientific and Technical Support Commission），組織概況如圖 2 所示。

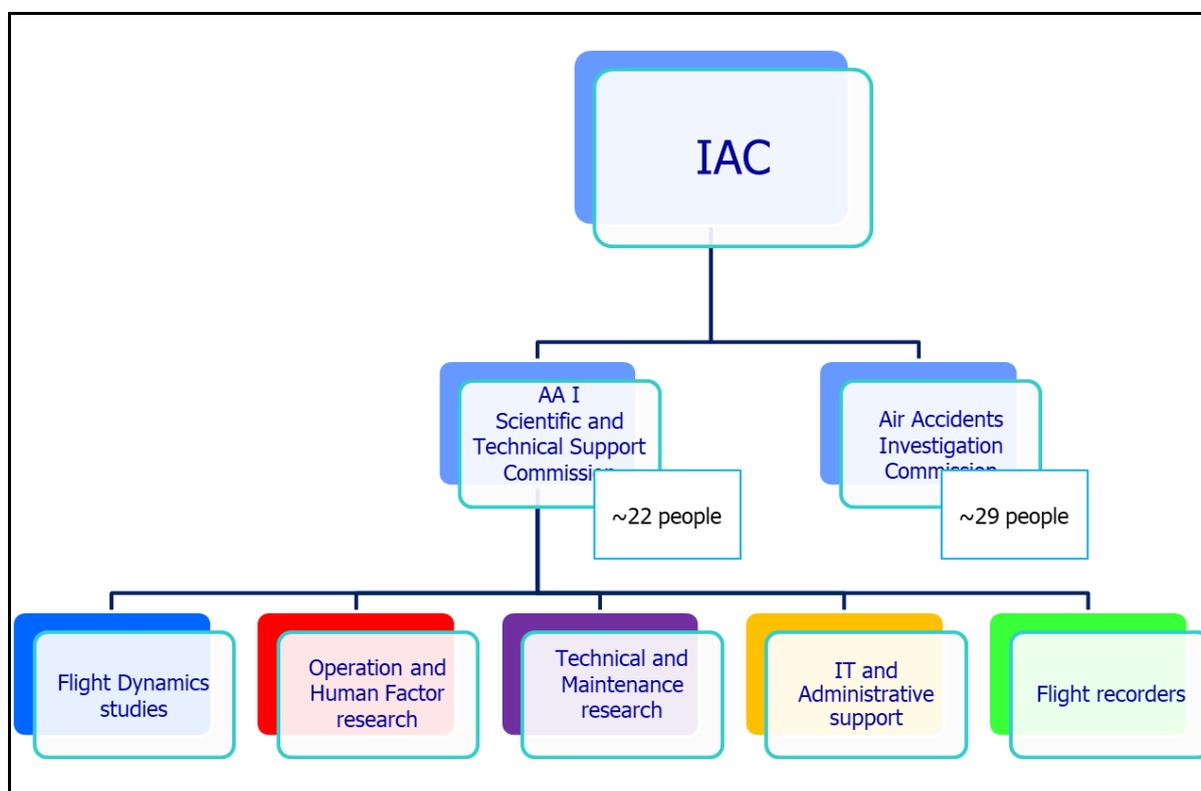


圖 2 IAC 飛航事故科學與技術支援委員會組織圖

此次在職訓練地點位於飛航事故科學與技術支援委員會於 2017 年經改建後新落成啟用之實驗室，相關配置如圖 2 所示，實驗室配置大致可分為四個區塊：

- A. 會議區（圖 3）：此區包括會議室、休息區、茶水間及盥洗室，會議室備有兩部大尺寸 50 吋 4K 畫質平面顯示器，能透過無線 HDMI 與電腦遠端連線，會議室與拆解區之間以玻璃牆區隔；平時提供實驗室人員開會討論、簡報及休息使用，事故發生時未參與紀錄器拆解之調查團隊成員仍可由此區觀察拆解區作

業情形，或在此同步進行其他辦公作業，休息區與茶水間可用以舒緩長時間作業之疲勞或提供簡單之輕便飲食。

- B. 拆解區（圖 4）：此區包括破壞工作區、鉗工作業區及主要拆解工作區，備有各式手工具、電動工具、空壓機、萬向節支架、燈架以及相機腳架以供各種拆解作業及拍照紀錄使用，角落設有洗手台以利裝備清洗或人員清潔作業，儲物櫃另外保存現場作業用之衛星測量儀器及兩套遙控無人機空拍系統。
- C. 飛航紀錄器下載工作區（圖 5）：此區主要負責一般民用航空器飛航紀錄器下載作業，所有工作區皆具備防靜電設置，包括歐美常見固態記憶體紀錄器以及俄製磁帶、鋼絲式紀錄器下載裝備，損壞紀錄器下載工具、座艙語音紀錄器錄音設備及資料下載工作站等，經處理後之損壞航電晶片亦於此進行資料下載作業，資料下載工作站與實驗室雲端系統相連，下載之資料可即時於專門的辦公室進行後續解讀作業。
- D. 損壞航電晶片處理工作區（圖 6）：此區主要負責損壞航電設備處理作業，所有工作區皆具備防靜電設置，包括光學電路放大鏡、30 倍率數位顯微鏡、紅外線晶片拆除與回焊工作站、焊接工作區、排氣櫃工作區及 X 光檢測系統，可支援各種 DIP、TSOP、BGA 及 eMMC 封裝晶片之拆焊、清潔、非破壞性檢測、植球及初步開蓋作業，X 光掃描儀除能進行晶片內部電路檢測之外，並可協助小型機械結構之內部檢視作業。

其中於損壞航電晶片處理之重點裝備分別介紹如下：

- 英國 PDR IR-E3 Evolution 可程式化回焊工作站（圖 7）：本體由 150W 紅外線元件加熱槍、2000W 電路板恆溫系統、元件真空吸取裝置及精密三軸工作平台為中心，搭配兩具紅外線數位溫度計與控制電腦連線，精密控制晶片加熱溫度以免於拆焊、回焊過程中損及晶片，工作平台並具備垂直攝影機及光學對位系統，除可簡單自電路板上拆下晶片之外，更可將已植球之 BGA 晶片與電路板上之腳位精確對位並焊回電路板上，完成電路板模組修復作業，大幅簡化損壞晶片解讀作業之流程。
- 德國 Feinfocus Y.Cougar SMT X 光檢測系統（圖 8）：加壓規格 160kV，具備 2,000x（幾何）至 10,000x（系統）放大倍率，並整合可傾斜三軸平台、CNC 控制及影像處理軟體，可即時快速檢視晶片內部之線路或元件，並選配 CT（斷層掃描三維重建）功能；IAC 表示整個實驗室環境皆通過認證以安裝此一 X 光系統，相關操作人員並需要受訓以取得 X 光系統操作資格，於未來將升級 CT 功能後進行其他工程技術支援之嘗試。
- 美國 TEEL Technologies（加拿大分公司）eMMC 晶片轉接器（圖 9）：對應主流 eMMC 及 eMCP 記憶晶片之 BGA 封裝，內建針腳可省去困難的晶片植球作業，同時因 eMMC 內建控制器，僅須將晶片腳位轉換為標準 SD 配接格式，

使用一般讀卡機即可直接下載晶片內之原始資料，而不需要經過客製化的下載裝備。

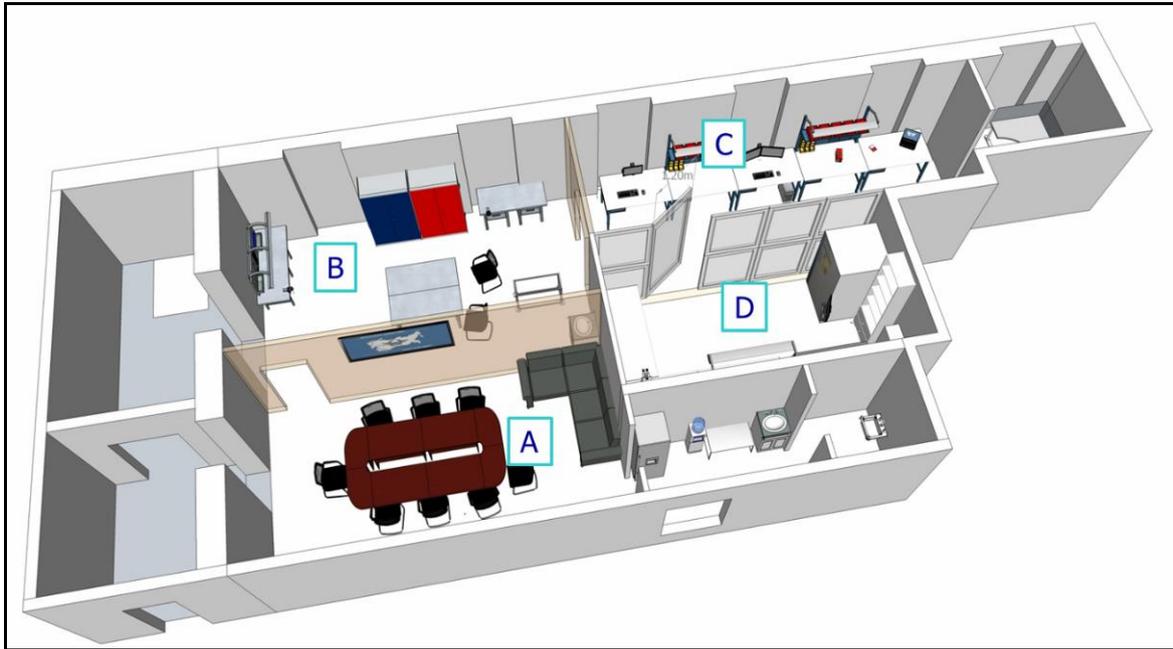


圖 2 IAC 實驗室配置圖



圖 3 實驗室會議區（小門後面為茶水間及盥洗室）



圖 4 透過會議區玻璃牆觀看之拆解區



圖 5 飛航紀錄器下載工作區



圖 6 損壞航電晶片處理工作區

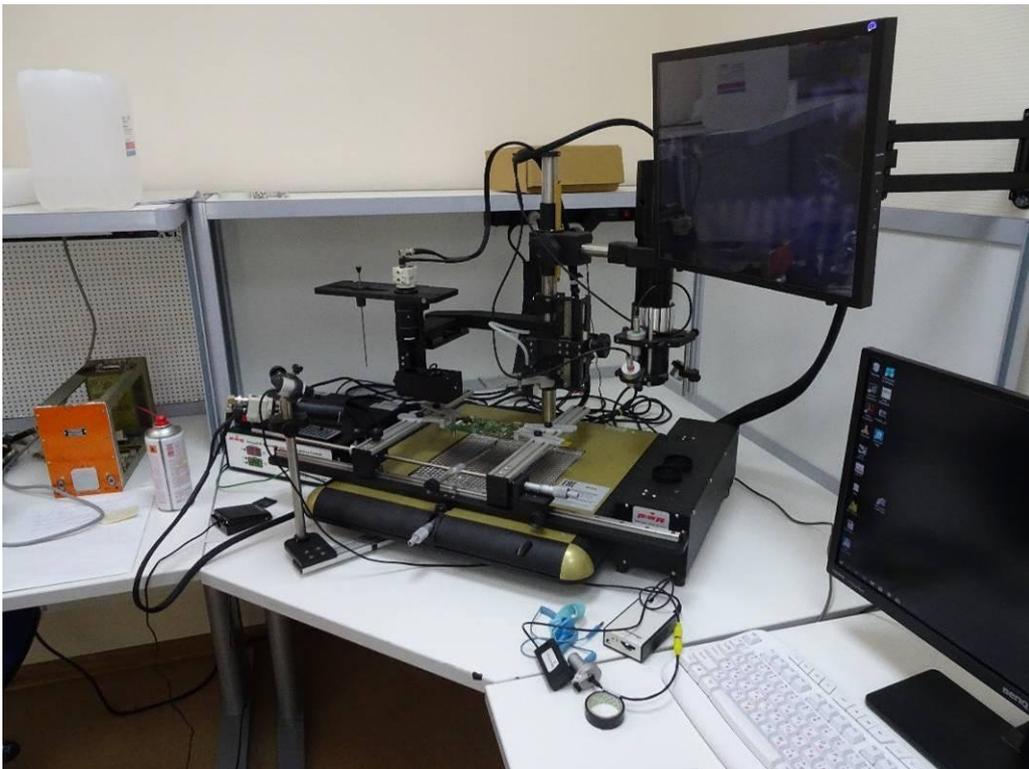


圖 7 紅外線晶片拆除與回焊工作站

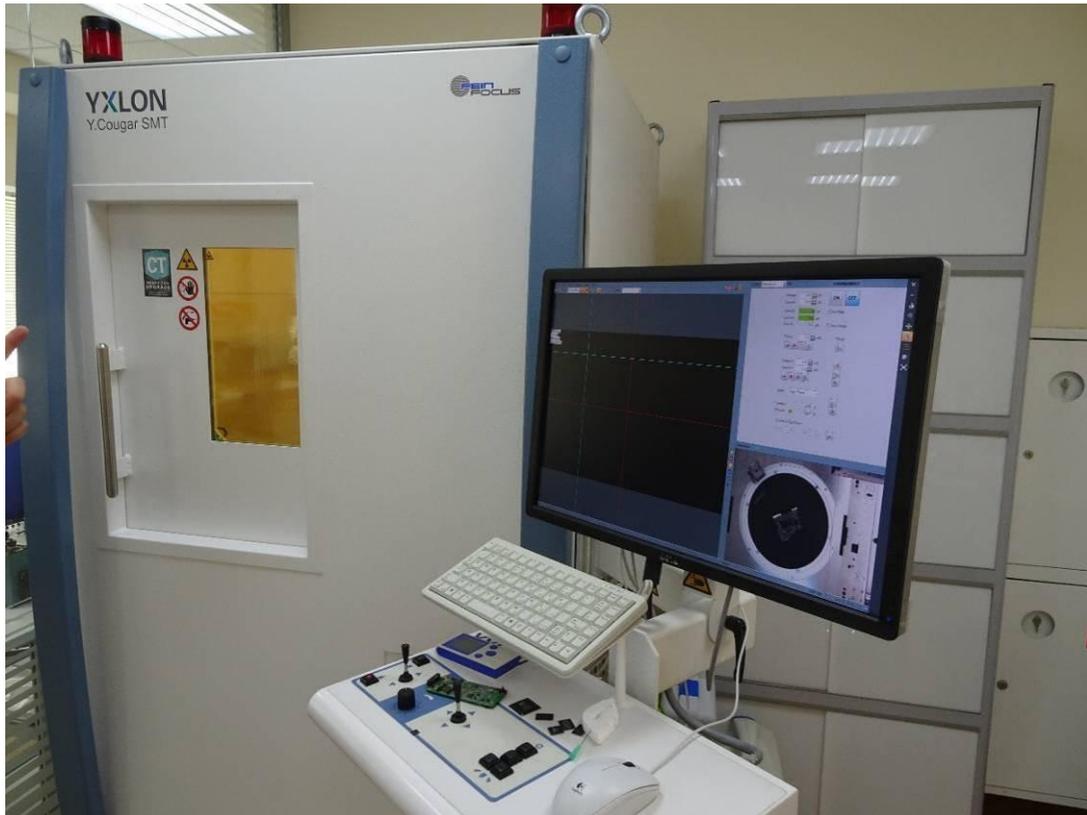


圖 8 X 光檢測系統



圖 9 eMMC 晶片轉接器

3.2. 損壞航電裝置硬體處理流程

依據 IAC 損壞晶片處理流程，航電裝置依據其損壞情形可大分為 4 類，並依據其損壞等級擬定不同之處理程序：

- 第 1 類：僅外觀損傷內部電路板無損且仍可正常開機，此類裝置等同於未損壞，以其原本之下載設備即可正常進行資料下載作業。
- 第 2 類：裝置外部螢幕、電源或其他介面受損，但記憶體所在之電路板模組無損，此類裝置可透過將記憶體模組轉接至另一部相同型號之裝置，依原本程序進行資料下載。
- 第 3 類：記憶體所在之電路板模組損傷，但記憶體晶片封裝無損傷，此類裝置需透過拆焊設備取下記憶體晶片，視其封裝（DIP、SOP、BGA）及記憶體種類（NOR、NAND 或 eMMC）使用對應之下載裝備（NOR、NAND 使用晶片燒錄器、eMMC 使用轉接器下載）進行晶片原始資料下載。
- 第 4 類：記憶體封裝受到物理損壞（火燒、變形、裂痕等），乃最嚴重之損傷種類，需以電路測試及 X 光檢測系統檢視封裝內部之晶體（Die）、線路以及其他元件之完整性，評估可行之救援方案，大部份為將封裝利用強酸溶穿至晶體與其接腳部位（開蓋），委託外部專業實驗室打線至新的轉接模組，重新封裝後再嘗試下載，此類處理最為耗費時間與經費成本。

上述第 1 類及第 2 類可以透過原廠之下載工具直接轉換出所需之參數，然而第 3 及第 4 類處理下載之原始資料為二進位原始碼，需透過分析解碼作業方能解讀。

3.3. 損壞航電裝置資料分析流程

IAC 利用自行開發之分析軟體 IAC HexView（如圖 10）進行原始資料之 GPS 軌跡分析解讀，HexView 以 16 進位方式檢視原始碼，並利用常見的編碼方式（ASCII 字碼、IEEE 浮點數或是 GPS 編碼）嘗試搜尋可能數據，標記並排序相關數據後，匯整並輸出 txt、GPS 或是 kml 檔案以還原飛航軌跡，其操作步驟如下：

1. 載入原始檔
2. 將大型檔案分切（針對超過 3GB 之原始檔）
3. 以 UTC 模組搜尋事故日期時間，標記時間參數
4. 手動刪除不需要的時間標記
5. 從時間標記前後搜尋經緯度及高度參數並標記
6. 輸出 txt、GPX 及 KML 檔



圖 10 IAC HexView 操作畫面

3.4. 損壞晶片解讀實作練習

本次訓練之重點在於實際操作損壞晶片解讀流程，以深入了解 IAC 之作業流程，因此學員本次特地攜帶一具本會曾實際調查之損壞手持式 GPS，做為此次實作之樣本，相關實作流程如下：

1. 損壞裝置模組拆解及清潔作業（圖 11）：將損壞裝置依原本構造拆解、清潔並進行拍照紀錄，在此階段同時進行損傷評估及確認記憶晶片所在位置及型號。
2. 記憶體晶片型號確認及外觀檢視作業（圖 12）：依同型航電裝置處理之經驗，IAC 講師穿戴防靜電綁帶後以手工具小心拆開主電路板模組上的電磁防護膜，內部存在主控制器晶片、記憶體晶片以及其他被動元件，從晶片上之型號查詢網路資料後判斷為 BGA 封裝之 eMMC 記憶體，雖然此一型號裝置為 IAC 首次接觸，但與相同製造商出品之相同系統裝製具備相似之配置，且晶片未有明顯物理損壞跡象，遂進行後續解讀流程。
3. 晶片 X 光內部檢視作業（圖 13）：X 光系統之操作必須由經過訓練並領有執照之人員執行，然為強化本次訓練成效，於進行安全提示之後，學員在 IAC 講師指導下學習使用 X 光檢測設備對樣本進行掃描，透過系統內建影像處理軟體及 CNC 控制平台對樣本進行 360 度檢視及 2.5D 傾斜放大檢視，確認電路板及晶片接點及晶片內部接線未有異常不連續情形，並完成相關紀錄後進行後續流程。
4. 晶片拆焊作業（圖 14）：使用紅外線晶片拆除與回焊工作站將晶片自電路板上取下，為整個作業中最高風險之階段，在拆焊過程中的溫度控制非常重要，需加熱至焊錫恰好融化卻又不損及晶片封裝之溫度，晶片在高溫中多曝露 1 秒鐘

都有可能導致內部資料的損傷，因此必須在一次的加熱循環中即能順利取下晶片；IAC 使用的回焊工作站具備紅外線感測回授可程式化控溫功能，並針對不同電路板的焊錫規格測試後建立對應不同設備所需的解焊溫度曲線；在進行焊接作業前先在晶片底下的縫隙間注入助焊劑，並須移除電路板上的電池以免晶片取下過程中晶片腳位電位改變造成內部資料受損。

5. 接點清潔作業（圖 15）：取下的 BGA 晶片以助焊劑、電烙鐵及吸錫器等手工具小心清理殘餘焊錫，需避免持續長時間加溫焊錫以免透過熱傳導損害內部晶片之資料。
6. 晶片資料下載作業（圖 16 及圖 17）：由於 eMMC 記憶體將控制器包含於晶片內部，在晶片狀況完好的情形下可以不透過其他外部控制器直接對晶片內之資料進行存取作業，因此將晶片放入 eMMC 轉接器後直接以 SD 讀卡機與電腦連線，Windows 系統即可將該晶片辨識為一外部儲存裝置，雖然因為晶片使用之格式非 Windows 格式無法直接存取檔案，但能透過磁碟下載工具如 Win32 Disk Imager 將晶片記憶體內之所有二進位原始資料下載，並進行後續解讀作業。
7. 晶片資料解讀作業（圖 18、圖 19 及圖 20）：使用 IAC HexView 開啟晶片原始檔，由於該晶片原始檔接近 4GB，包含該 GPS 裝置主要程式、背景圖資、各種設定、使用者拍攝照片、內存導航點及飛航軌跡等資料，為降低解析檔案處理所需之時間，需將檔案分切之後再針對存有飛航軌跡之部份進行解讀作業，講師依據他對該廠牌 GPS 裝置之解讀經驗，判斷飛航軌跡會存在最前面之部份，因此僅切出最前面 6.5MB 之檔案並分析，依據事故日期及其座標特定出資料特徵後解讀出事故當日之飛航軌跡，完成損壞裝置解讀作業。



圖 11 模組拆解及清潔

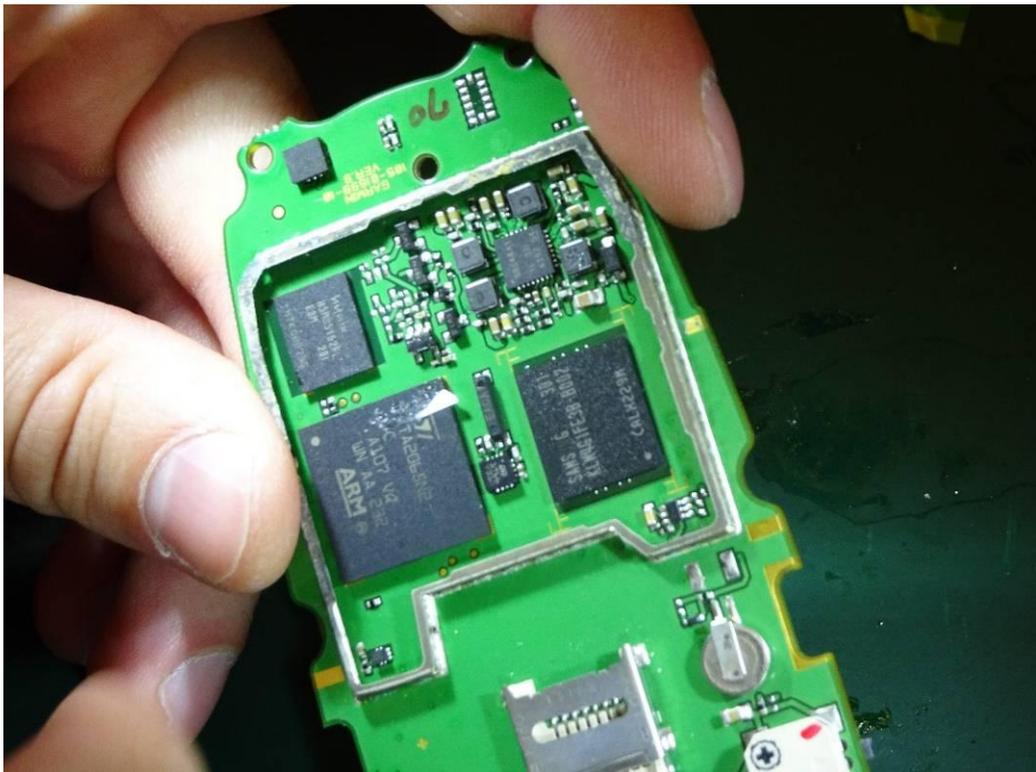


圖 12 記憶體晶片型號確認及外觀檢視



圖 13 X 光檢視晶片內部

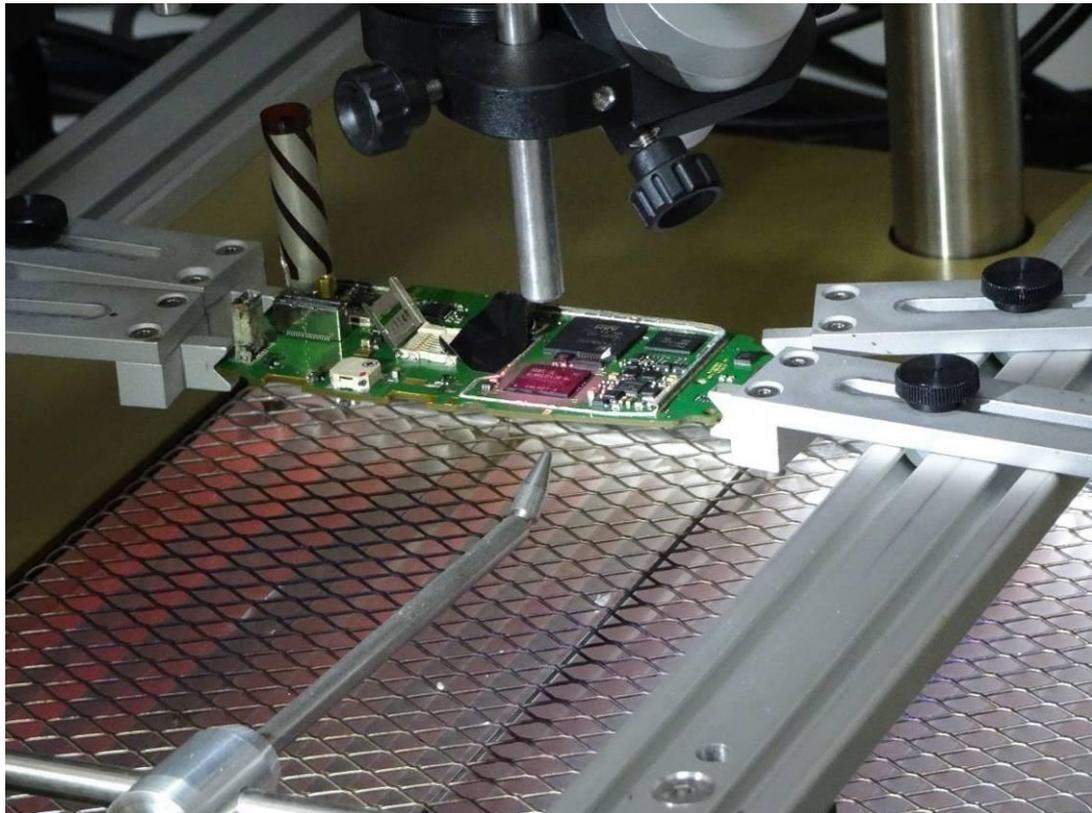


圖 14 晶片拆焊作業



圖 15 接點清潔作業

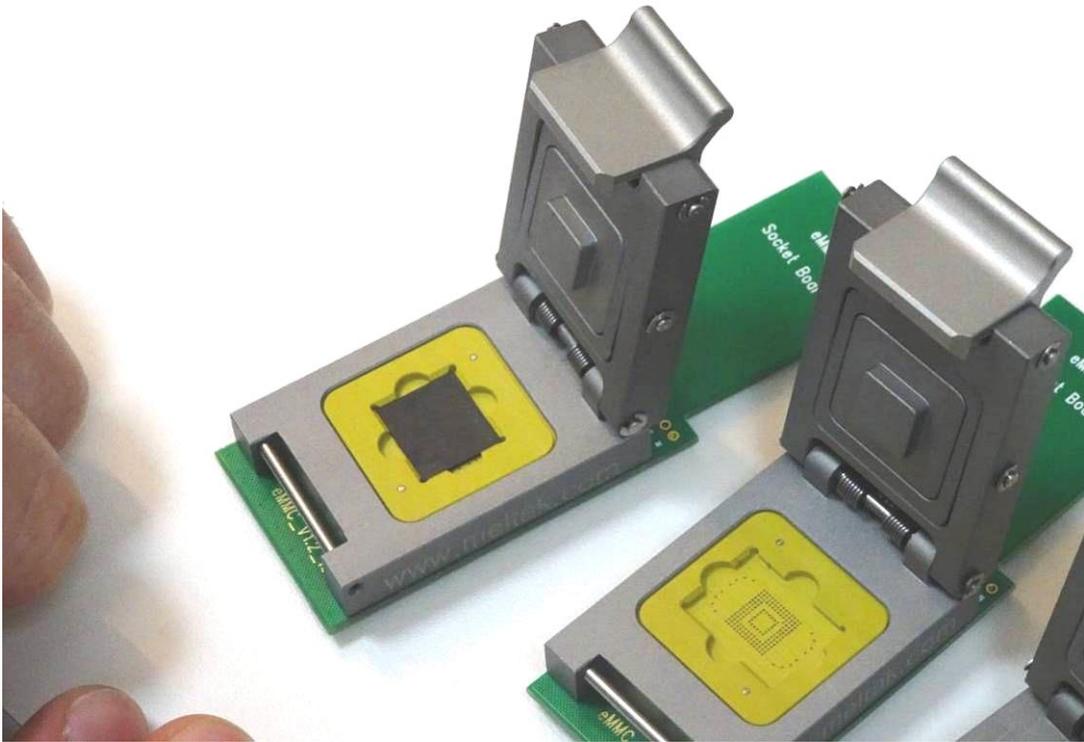


圖 16 置入 eMMC 晶片轉接器

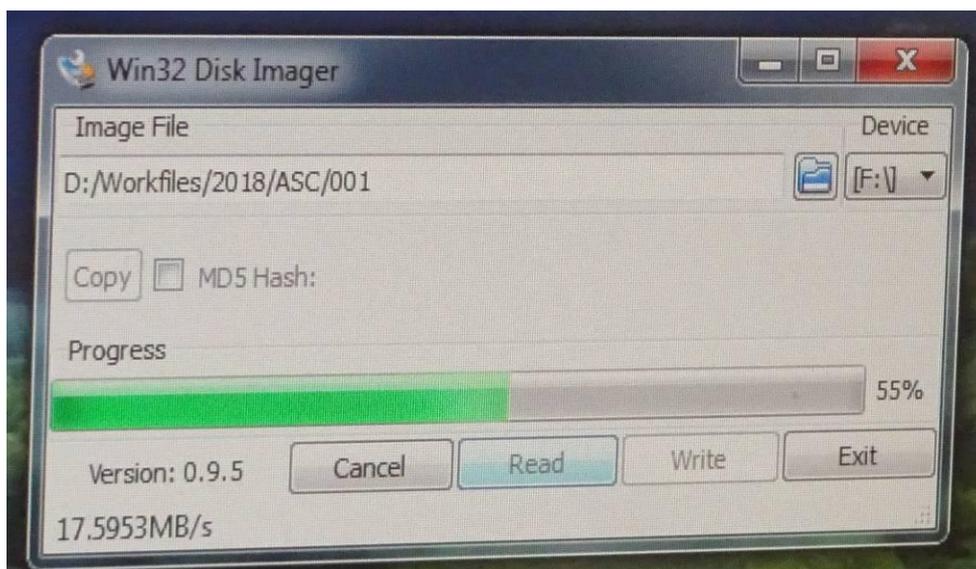


圖 17 原始資料下載

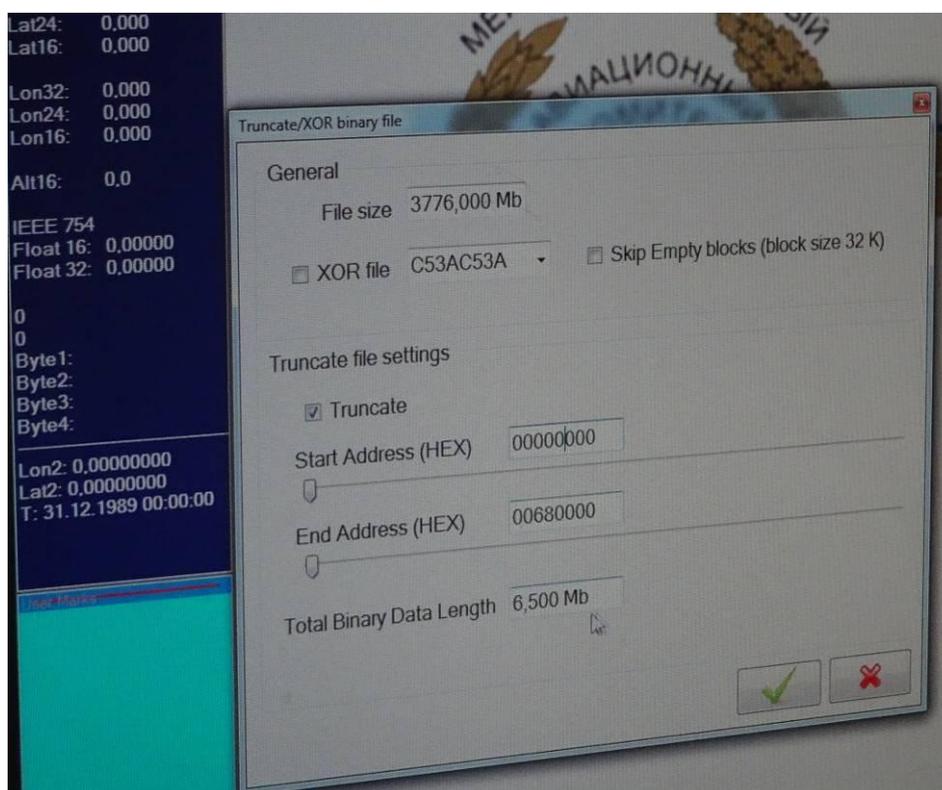


圖 18 檔案分切作業

3.5. 拜訪莫斯科國立無線電技術電子學與自動化科學技術大學奈米研究中心

IAC 為處理受到嚴重物理損壞的記憶體晶片，將其開蓋與修復作業委託莫斯科國立無線電技術電子學與自動化科學技術大學（Moscow Technical University - Moscow Institute of Radio Engineering, Electronics and Automation (MIREA)，圖 21）奈米研究中心協助處理，該校前身為 1947 年成立的全聯盟通訊電力研究所（All-Union Correspondence Power Institute），經過多年改制及與莫斯科多所理工院校合併之後而統稱為莫斯科技術大學，目前在莫斯科市內有 8 個校區，並有 4 座分校於莫斯科以外的俄羅斯境內，該校亦為歐洲頂尖工業管理者研究所（Top Industrial Managers for Europe, T.I.M.E.）聯盟成員，與 20 國 53 所聯盟學校之間互有碩博士雙學位學程計劃。

本次訓練期間，IAC 講師帶領本會學員前往該研究中心參觀並聽取簡報，該中心具備微晶片開蓋實驗室、微晶片打線實驗室、電路板熱風/紅外線拆焊設備、X 光檢測系統、穿隧式顯微鏡、雷射立體顯微鏡、晶體電子訊號探針系統、聚焦離子束電子束掃描式顯微鏡系統（FIB）及材料分析顯微鏡等設備，該中心除進行各種奈米微觀研究之外，並積極研究各式微晶片逆向工程修復及下載能量（圖 22），針對主要之記憶體晶片開發相對應之晶片下載設備（圖 23），本次參觀聽取之簡報為該中心近日幫 IAC 進行某俄製直昇機墜毀事故之損壞航電晶片記憶體下載作業，該晶片經 X 光檢測完成後開蓋修復晶體線路並下載晶片內之原始資料提供給 IAC 進行事故調查使用。



圖 21 MIREA 奈米研究中心所在之 Sokolinaya Gora Street 校區

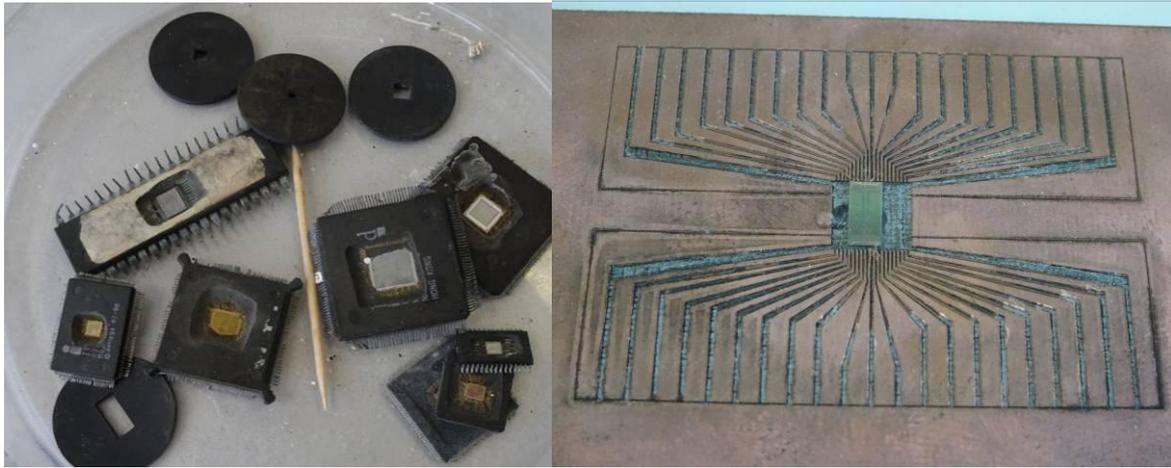


圖 22 該中心逆向工程研究之各式晶片樣本

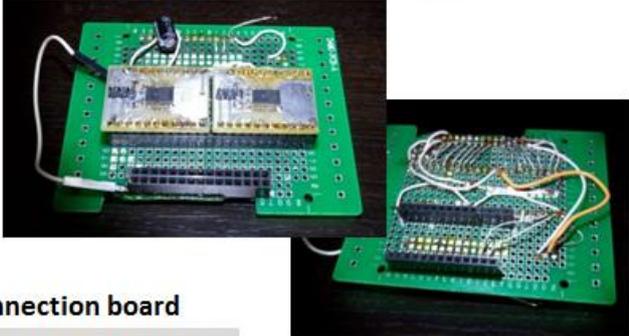
Universal Reader

Provide an ability to read Memory IC by eMMC interface (through controller chip) and test points (directly from memory chip).

Main module (FPGA)



Buffers and connection module



eMMC on connection board

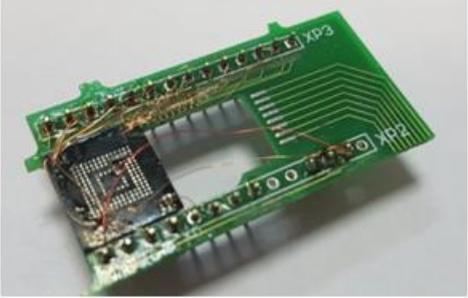


圖 23 該中心自行開發之晶片資料下載工具

四、心得及建議事項

本次訓練行程圓滿且收穫豐富，本次在職訓練雖著重於損壞裝置解讀能量，但 IAC 飛航事故科學與技術支援委員會於飛行動力學、飛航操作及人為因素、維修及系統技術等領域亦投注人力物力進行研究，且樂於與各國飛航事故調查單位分享其研究成果，於本次訓練期間更提供本會 HexView 解讀軟體的最新版本，在各專業領域皆值得本會持續學習，據此職提出 2 項建議：

1. 持續派員前往各國事故調查單位實驗室進行在職訓練，學習各國事故調查工程技術能量並維持技術合作。
2. 升級本會損壞航電晶片解讀能量以因應新式航電記憶晶片，並與國內相關單位接觸以交換經驗，建立嚴重物理損壞晶片救援管道。